CLAIMS

We claim:

Sub a1

1. A method of generating secure endorsed transactions comprised of transaction data representative of transactions and unique identifiers corresponding to parties endorsing the transactions, the method comprising the steps, performed by a data processing system, of:

receiving transaction data and unique identifiers; and

generating unique codes from the transaction data and unique identifiers, wherein the unique codes constitute secure endorsements of the transaction data by the parties corresponding to the unique identifiers.

2. The method of claim 1 wherein the generating step includes the substep of:

formatting the unique codes, the transaction data, and the unique identifiers to produce single whole representations of secure endorsed transactions.

a

3. The method of claim 1, wherein the data processing system includes a storage means, and wherein the generating step includes the substep of:

storing the unique codes, the transaction data, and the unique identifiers in the memory means.

4. The method of claim 2, wherein the data processing system includes a storage means, and wherein the formatting step includes the substep of:

storing the single whole representations of secure endorsed transactions in the ~~memory~~ storage means.

5. In a network comprised of point of sale (POS) equipment distributed remotely from a central controller, wherein the POS equipment includes a transaction input device and an identifier input device, a process for generating secure endorsed transactions comprising the steps, performed by the POS equipment, of:

receiving transaction input and unique human identifiers;

generating unique codes from the transaction data and unique human identifiers, wherein the unique codes constitute secure endorsements of the transaction data by the individuals corresponding to the unique human identifiers; and

transmitting the unique codes along with the transaction input and unique human identifiers to the central controller, wherein the unique codes, the transaction input, and the unique human identifiers constitute secure endorsed transactions.

6. The process of claim 5, wherein the central controller is connectable by a telecommunications network to the POS equipment, and wherein the transmitting step further includes the substep of:

linking the POS equipment to the telecommunications network.

7. The process of claim 6, wherein the central controller receives a signal indicating that the POS equipment has linked to the telecommunications network and wherein the linking substep further includes the sub-substep of:

sending the unique codes along with the transaction input and unique human identifiers to the central controller via the telecommunications network.

~~8. The process of claim 5, wherein the transmitting step includes the substep of:~~

~~formatting the unique codes, the transaction data, and the unique human identifiers to produce single whole representations of secure endorsed transactions.~~

9. The process of claim 8, wherein the central controller is connectable by a telecommunications network to the POS equipment, and wherein the transmitting step further includes the substep of:

linking the POS equipment to the telecommunications network.

10. The process of claim 9, wherein the central controller receives a signal indicating that the POS equipment has linked to the telecommunications network and wherein the linking substep further includes the sub-substep of:

sending the single whole representations of secure endorsed transactions to the central controller via the telecommunications network.

11. A method of generating forge-resistant, tamper-resistant secure endorsed transactions comprised of transaction data representative of transactions, unique human identifiers corresponding to at least one party, called first party, endorsing a transactions, and public keys corresponding to at least a second party endorsing a transaction, wherein the public keys have corresponding private keys maintained in secret by the second party, the method comprising the steps, performed by a data processing system, of:

receiving transaction data, a unique human identifier, and a public key;

generating a unique code from the transaction data, the unique human identifier, and the public key, wherein the unique code constitutes a secure endorsement of the transaction data by the first party; and

generating, using a private key corresponding to the received public key, a digital signature of the unique code, wherein the digital signature constitutes a secure endorsement of the transaction data by the second party.

12. The method of claim 11 wherein the second generating step includes the substep of:

formatting the digital signature, the transaction data, the unique human identifier, and public key to produce a single whole representation of the tamper-resistant secure endorsed transaction.

13. The method of claim 11, wherein the data processing system includes a storage means, and wherein the second generating step includes the substep of:

storing the digital signature, the transaction data, the unique human identifier, and the public key in the memory means.

14. The method of claim 12, wherein the data processing system includes a storage means, and wherein the formatting step includes the substep of:

storing the single whole representations of tamper-resistant secure endorsed transaction in the ~~memory~~ Storage means.

15. A method of verifying secure endorsed transactions comprised of transaction data representative of transactions, unique human identifiers corresponding to individuals endorsing the transactions, and unique codes generated from the transaction data and unique human identifiers, method comprising the steps, performed by a data processing system, of:

receiving secure endorsed transactions; and

generating unique codes from the transaction data and unique human identifiers of the secure endorsed transactions, wherein the unique codes constitute secure endorsements of the transaction data by the individuals corresponding to the unique human identifiers; and

comparing the unique codes of the received secure endorsed transactions with the generated unique codes to determine if there is a match, wherein if the unique codes of the received secure endorsed transactions match the generated unique codes then neither the transaction data nor unique human identifiers of the secure endorsed transactions have been altered prior to execution of the verification method.

16. In a network comprised of point of sale (POS) equipment distributed remotely from a central controller, wherein the POS equipment includes a transaction input device and an identifier input device, a process for verifying secure endorsed transactions having transaction data representative of transactions, unique identifiers corresponding to parties endorsing the transactions, and unique codes generated from the transaction data and unique identifiers, comprising the steps, performed by the POS equipment, of:

receiving secure endorsed transactions;

generating unique codes from the transaction data and unique identifiers of the secure endorsed transactions, wherein the unique codes constitute secure endorsements of the transaction data by the parties corresponding to the unique identifiers; and

comparing the unique codes of the received secure endorsed transactions with the generated unique codes to determine if they match, wherein if the unique codes of the received secure endorsed transactions match the generated unique codes then neither the transaction data nor unique identifiers of the secure endorsed transactions have been altered prior to execution of the verification process.

Sub a27

~~17. The process of claim 17, wherein the comparing step includes the substep of:~~

~~transmitting verification signals to the central controller indicating that neither the transaction data nor the unique identifiers of the secure endorsed transactions have been altered prior to execution of the verification process.~~

18. The process of claim 16, wherein the POS equipment includes an output display, and wherein the comparing step includes the substep of:

displaying verification messages indicating that neither the transaction data nor unique identifiers of the secure endorsed transactions have been altered prior to execution of the verification process.

19. A method of verifying a tamper-resistant secure endorsed transactions comprised of transaction data representative of a transaction, a unique identifier corresponding to at least one party, called a first party, endorsing the transaction, a public key corresponding to at least a second party endorsing the transaction, wherein the public key has a corresponding private key maintained in secret by the second party, and a digital signature generated using the private key corresponding to the public key, wherein the digital

signature constitutes an endorsement by the second party of the transaction, the method comprising the steps, performed by a data processing system, of:

receiving a tamper-resistant secure endorsed transaction;

generating a stored unique code from the digital signature and the public key of the tamper-resistant secure endorsed transaction;

generating a unique code from the public key, the human identifier, and the transaction data of the tamper-resistant secure endorsed transaction; and

comparing the unique code with the stored unique code to determine if they match, wherein if the stored unique code matches the generated unique code then neither the transaction data nor unique identifiers of the tamper-resistant secure endorsed transaction was altered prior to execution of the verification process.

20. The process of claim 5, wherein the POS equipment includes a smart card device for reading/writing card data for the transaction data from smart cards, wherein the receiving step includes the substeps of:

receiving signals from the smart card device indicating the insertion of smart cards; and acquiring card data from the inserted smart cards for inclusion in the transaction data.

21. The process of claim 20, wherein the transmitting step includes the substep of:

dispatching the secure endorsed transactions to the inserted smart cards.

22. The process of claim 20, wherein the transmitting step includes the substep of:

writing the secure endorsed transactions on the inserted smart cards.

23. In a network comprised of point of sale (POS) equipment distributed remotely from a central controller, wherein the POS equipment includes a transaction input device for receiving transaction input and an identifier input device for receiving unique identifiers optionally connectable to a smart card device for reading/writing card data from smart cards and writing data representative of secure endorsed transactions to smart cards, a process for generating secure endorsed transactions comprising the steps, performed by the POS equipment, of:

receiving a signal indicating insertion of a smart card in the smart card device;

reading card data from the inserted smart card;

receiving transaction input from the transaction input device;

combining the card data and transaction input to form a transaction data representative of a complete transaction;

receiving a human identifier from the identifier input device, the unique identifier corresponding to a party endorsing the complete transaction;

generating a unique code from the transaction data and the unique identifier, wherein the unique code constitutes an endorsement of the complete transaction by the party corresponding to the unique identifier; and

storing the unique code along with the transaction data and unique identifier on the smart card, wherein the unique code, the transaction data, and the unique identifier combined constitute a secure endorsed transaction.

Sub 93

24. A system for generating secure endorsed transactions having transaction data representative of transactions and unique identifiers corresponding to parties endorsing the transactions, the system comprising:

means for receiving transaction data and unique identifiers; and

43 cont

means for generating unique codes from the transaction data and unique identifiers, wherein the unique codes constitute secure endorsements of the transaction data by the parties corresponding to the unique identifiers.

25. The process of claim 1, wherein the data processing system includes a smart card device for reading/writing card data for the transaction data from smart cards wherein the receiving step includes the substeps of:

receiving signals from the smart card device indicating the insertion of a smart card; and

acquiring card data from the inserted smart card for inclusion in the transaction data.

26. The process of claim 25, wherein the transmitting step includes substep of:

dispatching the secure endorsed transaction to the inserted smart card.

27. The process of claim 26, wherein the transmitting step includes the substep of:

writing the secure endorsed transaction on the inserted smart card.

~~28. A method of generating transactions comprised of transaction receipt data representative of transactions, wherein a data processing system includes a smart card device for storing input transaction data and output transaction data, the method comprising the steps, perform by the data processing system, of;~~

~~receiving input transaction data from a smart card inserted in the smart card device;~~

~~generating output transaction data using the input transaction data; and~~

~~dispatching the output transaction data to the smart card.~~

29. The process of claim 11, wherein the data processing system includes a smart card device for reading/writing card data for the transaction data from smart cards wherein the receiving step includes the substeps of:

receiving signals from the smart card device indicating the insertion of a smart card; and

acquiring card data from the inserted smart card for inclusion in the transaction data.

30. The process of claim 29, wherein the transmitting step includes substep of:

dispatching the secure endorsed transaction to the inserted smart card.

31. The process of claim 30, wherein the transmitting step includes the substep of:

writing the secure endorsed transaction on the inserted smart card.